

ヒント:

次のことに関する質問があったので答えておきます。

ヒント 23.1. $K = \mathbb{Q}[\omega]$ とする。このとき、 $X^2 - 22$ は K 上 既約である。

はじめ聞かれたときには、とっさのことだったので、つぎのような証明を思い浮かべました。

[証明1] [略証: 使うときには自分で足りない部分を補足して使ってください。] $\mathbb{Z}[\omega]$ は ED で、それ故 PID で、UFD でもある。ガウスの補題が使えるから、 $X^2 - 22$ が $\mathbb{Z}[\omega]$ 上 既約であることを示せば良い。もし $X^2 - 22$ が $\mathbb{Z}[X]$ 上可約ならば、次数の関係から

$$X^2 - 22 = (aX + b)(cX + d) \quad (\exists a, b, c, d \in \mathbb{Z}[\omega])$$

である。 X の二次の項を比較することにより、 $ac(=ca) = 1$ なので、

$$\begin{aligned} X^2 - 22 &= (aX + b)(cX + d) = (aX + b)(ca)(cX + d) = ((aX + b)c) \cdot (a(cX + d)) \\ &= (X + bc)(X + ad) \end{aligned}$$

となるので、最初から $a = 1, c = 1$ として一般性を失わない。つまり

$$X^2 - 22 = (X + b)(X + d)$$

X の一次の項を考えれば、 $b + d = 0$ すなわち $d = -b$ で、それゆえ、

$$X^2 - 22 = (X + b)(X - b) = X^2 - b^2$$

である。 $b \in \mathbb{Z}[\omega]$ であったから、 $b = m + n\omega$ ($\exists m, n \in \mathbb{Z}$) である。

$22 = b^2 = m^2 + 2mn\omega + n^2\omega^2 = m^2 + 2mn\omega + n^2(-1 - \omega) = (m^2 - n^2) + (2mn - n^2)\omega$
 \mathbb{Q} 上 1 と ω は一次独立であるから、

$$(m - 2 - n^2) = 22 \text{ and } 2mn - n^2 = 0$$

後ろの式の方から、 $n = 0$ or $n = 2m$ が従うが、どちらも m, n が整数の解を持たないことがわかるから、このような b は存在せず、つまり $X^2 - 22$ は $\mathbb{Z}[\omega]$ 上可約であることがわかった。

... が、次のような証明のほうが体論らしいし、簡明でもある ($\mathbb{Z}[\omega]$ の環論も使わない) のでより優れていると思います。

[証明2] [略証: これも使うときは... 以下略] $X^2 - 22$ が K 上可約とすると、 $\sqrt{22} \in K$ である。すなわち $\mathbb{Q}[\sqrt{22}, \omega] = \mathbb{Q}[\omega]$, すなわち (この仮定の下では) $\mathbb{Q}[\omega]$ は $\sqrt{22}$ を含む \mathbb{Q} の拡大体である (2次拡大) ということになるが、 $\mathbb{Q}[\sqrt{22}]$ も $\sqrt{22}$ を含む体で、Gauss の補題を用いることにより \mathbb{Q} の2次拡大であることがわかる (\mathbb{Z} の環論)。 \mathbb{Q} 上の拡大次数の関係から $\mathbb{Q}[\sqrt{22}] = K$ でなければならない。ところが

$$\mathbb{R} \supset \mathbb{Q}[\sqrt{22}] = K \ni \omega \notin \mathbb{R}$$

となって、矛盾が生じる。 □

いずれにしても、どの体上考えるかが、議論に於いて大事で、それなしにはなににも言っていないのと変わらないのに注意してほしい。

◎「多項式 f が既約である」などというときは、必ず「 f は環 R 上既約である」などと土台になる環 R をつけて述べないと価値がないと言っています。

◎他にも、「最小多項式」「共役」なども、どの体上の話を書かないと同じ理由で意味がありません。